Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/CN05/000368

International filing date: 24 March 2005 (24.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: CN
Number: 200410017241.3
Filing date: 26 March 2004 (26.03.2004)

Date of receipt at the International Bureau: 24 May 2005 (24.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/CN2005/000368

证　　明

本证明之附件是向本局提交的下列专利申请副本

申　请　日：　2004.03.26

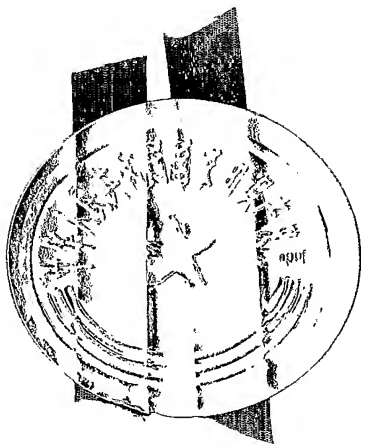
申　请　号：　200410017241.3

申请类别：　发明

发明创造名称：　具有指纹限制的机密文件访问授权系统

申　请　人：　上海山丽信息安全有限公司

发明人或设计人：　覃云川、周军刚



中华人民共和国
国家知识产权局局长　王景川

2005 年 4 月 12 日

权 利 要 求 书

1、一种具有指纹限制的机密文件访问授权系统，包括：

一授权服务器，其设有一授权模块，提供一指纹范本和一授权密钥；

一加密服务器，其设有一加密模块，接受所述授权模块所提供的授权密钥而产生一解密密钥，以及对待加密的机密文件予以加密而形成加密的机密文件；

一认证服务器，其设有一认证模块，接受所述授权模块所提供的指纹范本，接受所述加密模块提供的解密密钥，以及由客户机送来的请求认证的授权密钥，并判断确认提供认证解密密钥；以及

至少一客户机，每一客户机内设一用户模块，其在与其相应的客户机的操作系统内核嵌入内核加密/解密单元，接受所述授权模块提供的授权密钥并送认证模块请求认证，经认证模块认证后返回认证的解密密钥而开启所述的加密/解密单元，对加密的机密文件予以读出/写入。

2、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于，所述的授权服务器、加密服务器和认证服务器合并成一个系统服务器，其内设置所述的授权模块、加密模块和认证模块。

3、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权服务器和加密服务器合并成一个授权与加密服务器，其内设置所述的授权模块和加密模块。

4、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权服务器和认证服务器合并成一个授权与认证服务器，其内设置所述的授权模块和认证模块。

5、根据权利要求 1 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密服务器和认证服务器合并成一个加密与认证服务器，其内设置所述的加密模块和认证模块。

6、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述授权模块包括：平行设置的一口令指纹单元、一环境指纹采集单元和一时间指纹采集单元，以及分别与该平行设置前三个单元成双向程序链接的授权单元；该授权单元提供授权密钥；而该平行设置的口令指纹单元、环境指纹采集单元和时间指纹采集单元则汇合提供指纹范本。

7、根据权利要求 6 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权密钥是一个具有一定长度的二进制数串。

8、根据权利要求 7 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的授权密钥可以放入具有授权实体之中。

9、根据权利要求 6 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述的指纹范本是一个具有一定长度的二进制数串。

10、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密模块包括依次成程序联结的密钥产生单元和加密单元；该密钥产生单元接受来自授权模块提供的授权密钥后提供解密密钥；该加密单元接受待加密的机密文件输入并使用密钥产生单元提供的解密密钥而产生加密后的机密文件。

11、根据权利要求 10 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密单元接受待加密的机密文件输入并使用所述授权密钥产生加密机密文件。

12、根据权利要求 10 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述加密单元接受待加密的机密文件输入并同时使用所述的解密密钥和授权密钥而产生加密机密文件。

13、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述认证模块包括接受所述授权模块提供的指纹范本而平行设置的一环境指纹认证单元、一口令指纹认证单元和一时间指纹认证单元；以及与它们成双向程序联结的认证接口单元，该认证接口单元还分别接受所述加密模块提供的解密密钥和用户模块送来的请求认证的授权密钥，

接受所述加密模块提供的解密密钥和用户模块送来的请求认证的授权密钥，以及向用户模块提供认证的解密密钥。

14、根据权利要求 1～5 中任一项所述的具有指纹限制的机密文件访问授权系统，其特征在于所述用户模块包括依次成双向程序联结的应用程序单元、内核加密/解密单元和输入输出单元；以及接受授权模块提供的授权密钥并将其送入该内核加密/解密单元的授权输入单元；该内核加密/解密单元向所述认证模块提供请求认证的授权密钥和接受由所述认证模块送来的认证的解密密钥；以及该输入输出单元双向连接加密机密文件；该内核加密/解密单元嵌置于所述客户机操作系统内核。

15、根据权利要求 14 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述客户机操作系统为 Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server 或 Linux/Unix 或 Pocket, Symbian OS, Windows CE 嵌入式操作系统或 Mac OS 或 Sun OS, Novell netware 及其它服务器或网络操作系统。

16、根据权利要求 14 所述的具有指纹限制的机密文件访问授权系统，其特征在于所述应用程序单元的程序可以是 Microsoft Office 及其组件或其它桌面应用程序或嵌入式应用程序。

说 明 书

具有指纹限制的机密文件访问授权系统

技术领域

本发明涉及一种信息安全技术，具体地说，是一种具有环境限制和时间限制的机密文件访问授权的系统。

背景技术

现有的机密文件访问授权系统不具有环境限制和时间限制的机密文件访问授权功能，以文件保险箱技术为例，它在计算机中建立一个加密的存储区以存放机密文件，使用者必须持有授权密钥才能访问该加密存储区中的机密文件。但是，当使用者将该机密文件复制到其它电脑，则任何人无须密钥即可访问。如图 1 所示，其示出 PGPDISK 保护下的文件可以拷贝到未加密的磁盘 B，磁盘 B 可以被带到任何地方，从而失去权限控制。很明显，PGPDISK 的加密/解密没有环境限制，也就是说即使带走的文件是加密的，那么，在另一个地方，只要安装 PGPDISK 软件，也就可以访问该加密文件。

另一种现有技术是机密文件加密技术。被加密的机密文件只有持有授权密钥才能访问。然而，如果该机密文件被持有者转移到非法环境，例如，盗取到家中或盗取到异国它乡，由于持有授权密钥，持有者仍然可以访问该机密文件。换言之，机密文件的授权需要一种“在位授权”机制，即是说，机密文件的授权对象必须在某个职位上或在某种条件下才拥有访问机密文件的权限，一旦授权对象的职位发生改变或者其授权条件消失，他就不应该再持有访问该机密文件的权限。现有访问授权技术无法做到这一点。

发明内容

如上所述，如何克服现有机密文件访问授权系统存在机密文件被非法盗

取的缺陷，乃是本发明所要解决的技术问题，为此，本发明的目的之一是将对机密文件的访问授权限制在特定环境内。特定环境可以是单台台式电脑，单台笔记本电脑，单台掌上电脑,智能电器的计算单元，含有嵌入式计算芯片的设备，以及由上述电脑,电器或设备构成的一定范围的局域网，广域网或互联网及其它数字网络体系。通过本发明提供的技术，管理员可指定授权有效的环境，在该环境之外，指定的机密文件不可访问。

本发明的另一个目的是将对机密文件的访问授权限制在一定时间内，一定时间可以是从当前时间开始计算的一个时间段，例如几小时,几天,几星期,几月等。一定时间还可以是不依赖当前时间的独立时间段，例如星期五上午8:00 到下午 5:30，1 月 1 日到 1 月 31 日等.通过本发明提供的技术，管理员可指定授权有效的一定时间,在指定的有效时间之外，指定的机密文件不可访问。

把上述的本发明目的所确定的环境限制与时间限制进行整合成指纹限制，则本发明的总的目的在于提供一种具有指纹限制的机密文件授权访问系统。

本发明的技术解决方案如下：

根据本发明的一种具有指纹限制的机密文件访问授权系统，包括：一授权服务器，其设有一授权模块，提供一指纹范本和一授权密钥；一加密服务器，其设有一加密模块，接受所述授权模块所提供的授权器钥而产生一解密密钥，以及对待加密的机密文件予以加密而形成加密的机密文件；一认证服务器，其设有一认证模块，接受所述授权模块所提供的指纹范本，和接受所述加密模块提供的解密密钥，以及由客户机送来的请求认证的授权密钥，并判断确认向客户机提供认证的解密密钥；以及至少一客户机，每一客户机内设一用户模块,其在与其相应的客户机的操作系统内核嵌入内核加密/解密单元，接受所述授权模块提供的授权密钥，并将该授权密钥送所述认证模块请求认证，经认证模块认证后返回认证的解密密钥而开启所述的加密/解密单元，对加密的机密文件予以读出和写入操作。

所述授权服务器、加密服务器和认证服务器可以合并成一个系统服务器，其设有相应的授权模块、加密模块和认证模块；授权模块提供指纹范本和授权密钥；加密模块接受授权密钥并对待加密机密文件予以加密而形成加密机密文件，以及提供解密密钥；认证模块接受所述指纹范本，以及解密密钥，并和所述用户模块连接，接受用户模块送来的授权密钥请求，并予判断而给用户模块返回认证授权密钥与认证解密密钥；

所述授权服务器和加密服务器合并成一个授权与加密服务器，该授权与加密服务器设有授权模块和加密模块，并由授权与加密服务器提供授权密钥、指纹范本、解密密钥以及对待加密机密文件予以加密并形成加密机密文件，并分别与认证服务器的认证模块及客户机的用户模块相联结；

所述授权服务器与认证服务器相结成授权与认证服务器，其内设有的授权模块和认证模块，并分别向加密服务器内的加密模块和向客户机的用户模块提供授权密钥，以及接受客户机的用户模块送来的请求认证其所接受授权密钥，同时返回认证授权密钥和认证解密密钥。

所述的加密服务器与所述的认证服务器结合成一个加密与认证服务器，其内设有加密模块和认证模块；该加密模块接受来自授权服务器所提供的授权密钥而对待加密机密文件予以加密而形成加密机密文件；以及提供解密密钥送该认证模块，再由该认证模块向客户机的用户模块提供认证解密密钥允许客户机进行读出/写入加密机密文件的运作。

进一步，所述授权模块包括：平行设置的口令指纹单元、环境指纹采集单元和时间指纹采集单元，以及后接它们的授权单元，并由该授权单元提供授权密钥和所述的平行设置前三个单元汇集提供指纹范本。所述的指纹范本是一个具有一定长度的二进制数串，其含有口令和环境指纹信息；或含有口令和时间指纹信息；或含有口令、环境指纹和时间指纹信息。所述授权密钥是一个具有一定长度的二进制数串，并可以放入具有授权的实体之中；

所述加密模块包括依次成程序联结的密钥产生单元和加密单元；该密钥产生单元接受授权模块提供的授权密钥后提供解密密钥；该加密单元接受待

加密的机密文件的输入并使用密钥产生单元提供的解密密钥产生加密机密文件或使用授权密钥对待加密机密文件形成加密机密文件；或使用解密密钥和授权密钥来形成加密机密文件；

所述的认证模块包括接受所述授权模块提供的指纹范本而平行设置的环境指纹认证单元、口令指纹认证单元和时间指纹认证单元；以及与它们成双向程序联结的认证接口单元，该认证接口单元还分别接受所述加密模块提供的解密密钥和用户模块送来的请求认证的授权密钥，以及向用户模块提供认证的解密密钥；

所述的客户机用户模块包括依次成双向程序联结的应用程序单元、内核加密/解密单元和输入输出单元；以及接受授权模块提供的授权密钥并将其送入该内核加密/解密单元的授权输入单元；该内核加密/解密单元向所述认证模块提供请求认证的授权密钥和接受由所述认证模块送来的认证的解密密钥；以及该输入输出单元双向连接加密机密文件；该内核加密/解密单元嵌置于所述客户机操作系统内核（操作文件）。更具体地，客户机操作系统为Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server或Linux/Unix或Pocket, Symbian OS, Windows CE 嵌入式操作系统或 Mac OS 或 Sun OS, Novell netware 及其它服务器或网络操作系统。所述应用程序单元的程序可以是Microsoft Office 及其组件或其它桌面应用程序或嵌入式应用程序。

如上所述，本发明的信息安全比现有技术有着实质性的提高，其对机密文件的访问授权受到环境限制和时间限制。

附图说明

图 1 是现有的 PGPDISK 的加密保护示意图。

图 2 是本发明的环境加密保护示意图。

图 3 是本发明的授权模块结构示意图；

图 4 是本发明的加密模块结构示意图；

图 5 是本发明的认证模块结构示意图；

图 6 是本发明的用户模块结构示意图；

图 7 是本发明的系统结构示意图。

具体实施方式

下面根据图 2～7 给出本发明的较好实施例，并予以详细描述，并结合对实施例的阐述，进一步提供本发明的技术细节，使能更好地理解本发明的技术特征和功能特点，但都是为了说明本发明，而不是用以限制本发明的保护范围。

请参阅图 2，其显示本发明的技术方案的构思，即对所有的 I/O 通道（例如所有的机密文件载体之磁盘，光盘，网络，文件，网页等等）进行加密保护，使得不会有未加密的文件被带走；其加解密必须在指定的环境中进行（环境指纹）认证，因此，即使加密文件被带走，由于在另一个地方（环境）无法获得合法的环境指纹，从而无法通过环境认证，这样，盗用者仍然无法打开使用加密文件。

按图 2 所示的技术构思，提供典型实施例：

如图 3 所示本发明的系统中具有一授权服务器 1 其设有：一授权模块 10，上述授权模块 10 具有平行设置的一口令指纹单元 101、一环境指纹采集单元 102 和一时间指纹采集单元 103、以及一后接它们的授权单元 104。上述口令指纹单元 101 根据指定口令产生具有唯一性和不可复制性的数据作为口令指纹。上述环境指纹采集单元 102 从指定环境中采集具有唯一性和不可复制性的数据作为上述环境的指纹。上述具有唯一性和不可复制性的数据可以是网卡 MAC 地址，可以是硬盘的序列号。上述时间指纹采集单元 103 根据当前时间和管理者指定的时间限制生成具有唯一性和不可复制性的数据作为时间指纹。上述授权单元 104 根据上述口令指纹单元 101 生成的口令指纹，与根据上述环境指纹采集单元 102 采集到的环境指纹，或与根据上述时间指纹单元 103 生成的时间指纹，生成具有唯一性和不可复制性的授权密钥 5。上述具有唯一性和不可复制性的授权密钥 5 是一个具有一定长度的二进制数

串。它可以放入具体的授权实体中。上述授权实体具有的表现形式可以是：密码，电子钥匙，数字证书，加密狗及其它具有防犯非法复制功能的硬件或软件。同时，上述口令指纹单元 101 生成的口令指纹，上述环境指纹采集单元 102 采集到的环境指纹，以及上述时间指纹单元 103 生成的时间指纹，可以合并放入一指纹范本 6。在后面将要讨论的认证模块中，以上述指纹范本与待认证指纹进行比较，从而根据比较结果确定认证结果。上述指纹范本 6 是一个具有一定长度的二进制数串。

如图 4 所示，本发明的系统中具有一加密服务器 2，其设有一加密模块 20，上述加密模块 20 具有一密钥产生单元 201 和一加密单元 202，它们依次以程序联结。上述密钥产生单元 201 使用来自上述授权模块 10 提供的授权密钥 5 产生解密密钥 7。上述加密单元 202 使用上述授权密钥 5 和上述解密密钥 7，或仅使用其中之一，对待加密的机密文件 8 执行加密过程，生成加密后的机密文件 9。上述加密过程可以采用公钥方法，也可以采用私钥方法。上述加密后的机密文件 9 可以公开发布。

如图 5 所示，本发明的系统中具有一认证服务器 3，其设有一认证模块 30。上述认证模块 30 设有平行配置的一环境指纹认证单元 301、一口令指纹认证单元 302 和一时间指纹认证单元 303，以及分别与它们成双向程序联结的一认证接口单元 304。上述环境指纹认证单元 301，上述口令指纹认证单元 302，以及上述时间指纹认证单元 303，分别从上述授权模块 10 提供的指纹范本 6 中取得环境指纹范本，口令指纹范本和时间指纹范本。以及，上述环境指纹认证单元 301，上述口令指纹认证单元 302，以及上述时间指纹认证单元 303，通过上述认证接口单元 304 分别从后面图 6 要描述的客户机 4 送出的送认证的授权密钥 5’中取得待认证的环境指纹，口令指纹和时间指纹。认证过程为，上述环境指纹认证单元 301 比较上述环境指纹范本和上述待认证环境指纹，并把比较结果返回给上述认证接口单元 304。上述口令指纹认证单元 302 比较上述口令指纹范本和上述待认证口令指纹，并把比较结果返回给上述认证接口单元 304。上述时间指纹认证单元 303 比较上述时间

指纹范本和上述待认证时间指纹，并把比较结果返回给上述认证接口单元304。上述认证接口单元 304 根据上述三个比较结果判断，如果三个结果都是相同则认证成功，否则认证失败。并且只在认证成功的情况下，上述认证接口单元 304 将会把来自上述加密模块 20 提供的解密密钥 7 生成认证的解密密钥 7’送给请求认证的用户模块 40，用户模块 40 方可以此认证解密密钥 7’解密已加密的机密文件 9（参见图 6）。

如图 6 所示，本发明的系统中具有至少一客户机 4，每一客户机 4 设有一用户模块 40。上述用户模块 40 具有依次成程序联结的一授权输入单元 401，和一内核加密/解密单元 402；该内核加密/解密单元 402 分别与一输入输出单元 403 成双向联结，和与一应用程序单元 404 成双向程序联结。上述授权输入单元 401 接受用户输入的上述授权实体，并从上述授权实体中取出其中含有的授权密钥 5,并将该授权密钥 5 传递给上述内核加密/解密单元 402。上述内核加密/解密单元 402 连接上述认证模块 30 之认证接口单元 304，并提交上述授权密钥 5 请求认证。如果认证通过，则从上述认证模块 30 之认证接口单元 304 获得解密所必须的上述认证的解密密钥 7’。上述内核加解密单元 402 系无缝嵌入在操作系统内核及应用程序内核，从而能用上述授权密钥 5 和上述认证的解密密钥 7’对所有读进和写入的上述加密后的机密文件 9 进行加密/解密动作。如果授权无效，则认证必定失败，则上述内核加解密单元 402 不能取得上述认证的解密密钥 7’，从而无法解密上述加密后的机密文件 9，从而使之不可访问。上述操作系统可为 Microsoft Windows 95/98/ME/NT/2000/XP/2003 Server.上述操作系统可以是 Linux/Unix 操作系统；上述操作系统可以是 Pocket, Symbian OS, Windows CE 等嵌入式操作系统；上述操作系统可以是 Mac OS；上述操作系统可以是 Sun OS，Novell netware 及其它服务器或网络操作系统。上述应用程序可以是 Microsoft Office 及其组件；上述应用程序可以是其它桌面应用程序或嵌入式应用程序。

如上所述，本实施例系统的组成包括：一授权服务器 1，内设授权模块 10；一加密服务器 2，内设加密模块 20；一认证服务器 3，内设认证模块 30；

以及至少一客户机 4，每一客户机 4 内设用户模块 40，所述的授权模块 10、加密模块 20 和认证模块 30，以及用户模块 40 它们的连接关系则如图 5 所示，所述的授权模块 10 提供指纹范本 6 送认证模块 30；提供授权指纹 5 分别送加密模块 20 和用户模块 40；加密模块 20 对待加密的机密文件 8 进行加密而形成加密的的机密文件 9，并向认证模块 30 提供解密密钥 7；认证模块 30 接受指纹范本 6、解密密钥 7，以及由用户模块 40 送来的请求认证授权指纹 5'，经确认授权指纹 5' 后向用户模块 40 返回经认证的解密密钥 7' 用户模块 40 获得认证模块 30 送来的认证解密密钥 7' 后使设在客户机 4 的操作系统内核（文件系统）的内核加密/解密单元 402 动作而允许对加密机密文件 9 进行读出和写入。

作为上述实施例的替换，授权服务器 1、加密服务器 2 和认证服务器 3 可以合并而由一只系统服务器来取代，并在该系统工程服务器内设置授权模块 10、加密模块 20 和认证模块 30，它们的内部设置以及相互联结则仍照上述实施例。

当然，也可采用把加密服务器 2 与授权服务 1 合并且分别设置相应的加密模块 20 和授权模块 10，而认证服务器 3 为独立体，并内设认证模块 30。

说 明 书 附 图

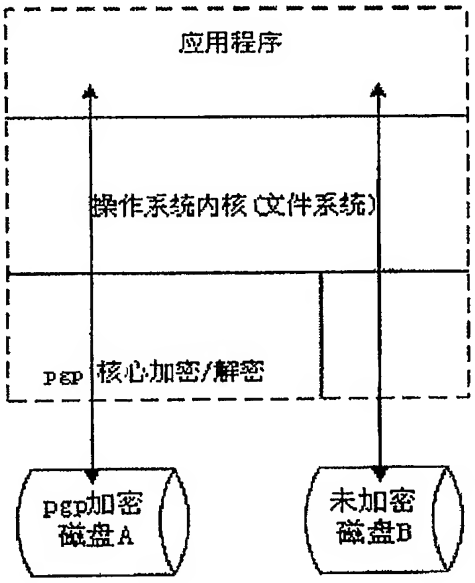

应用程序
操作系统内核（文件系统）
pgp 核心加密/解密
pgp加密
磁盘A
未加密
磁盘B

图1

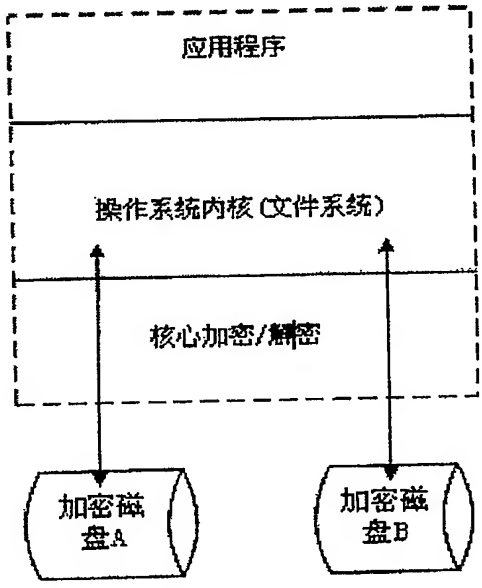

应用程序
操作系统内核（文件系统）
核心加密/解密
加密磁
盘A
加密磁
盘B

图2

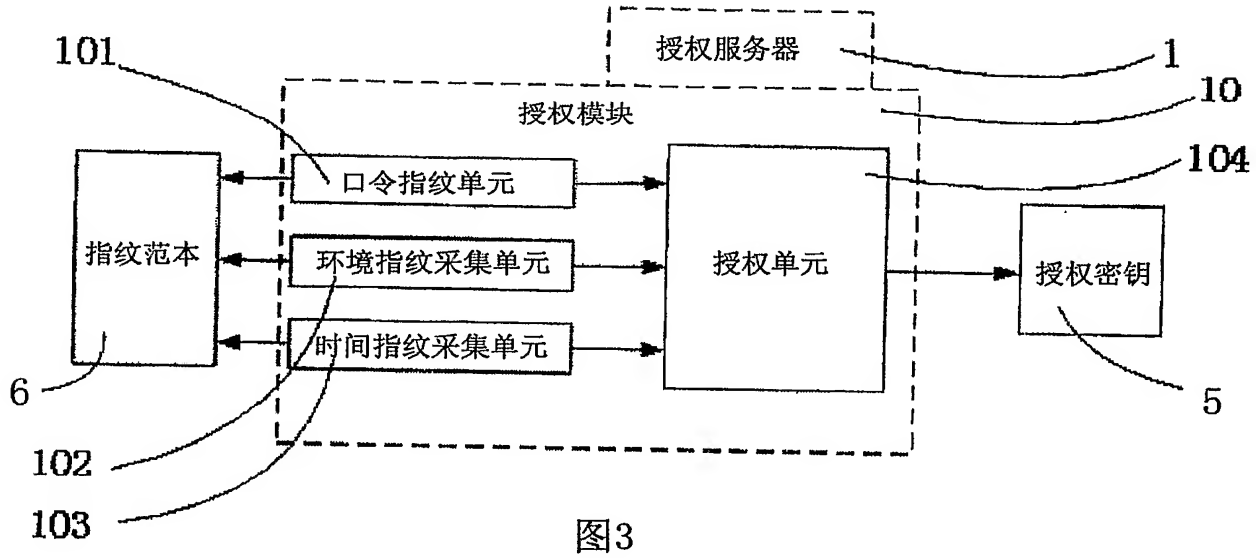

授权服务器
1
101
授权模块
10
口令指纹单元
104
指纹范本
环境指纹采集单元
授权单元
授权密钥
时间指纹采集单元
6
5
102
103

图3

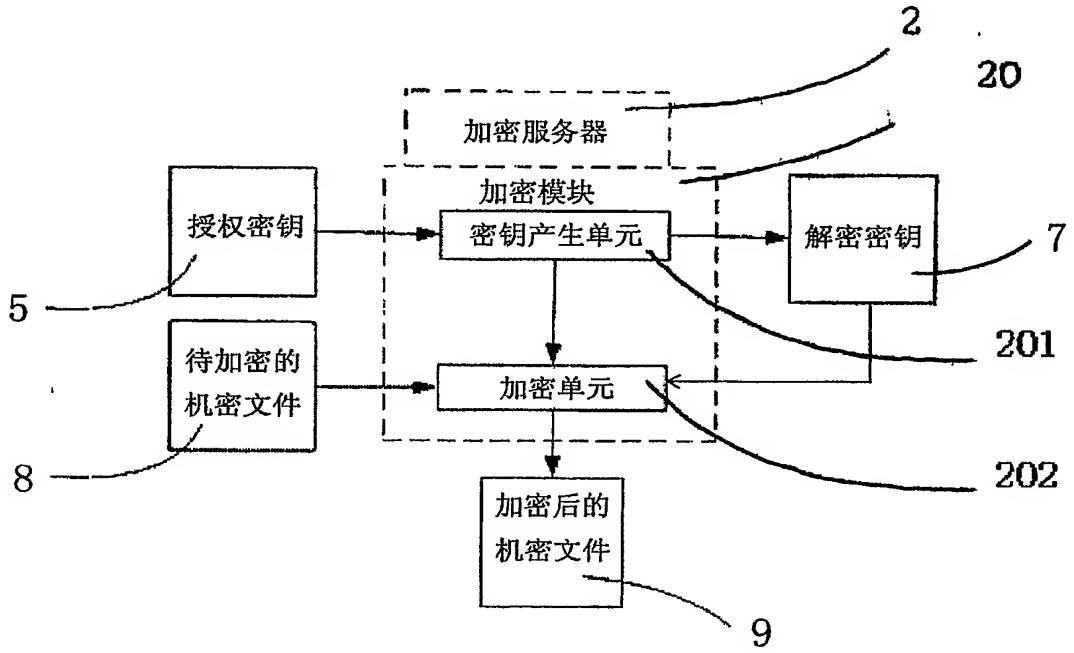

2
20
加密服务器
加密模块
授权密钥
密钥产生单元
解密密钥
7
5
201
待加密的
机密文件
加密单元
8
202
加密后的
机密文件
9

图4

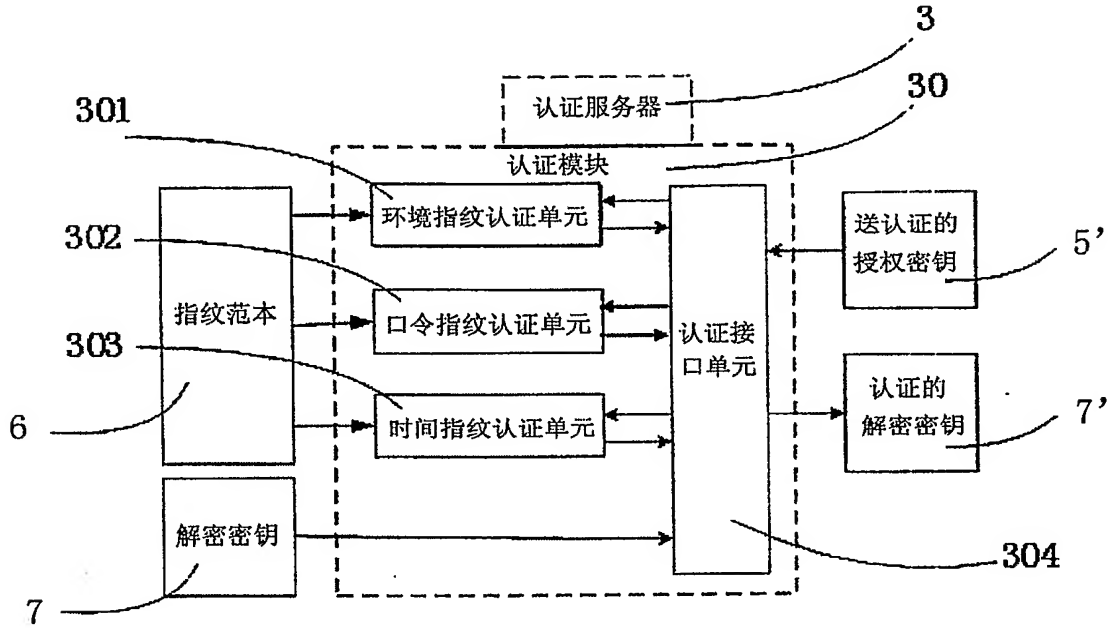

3
认证服务器
30
301
认证模块
环境指纹认证单元
302
口令指纹认证单元
303
时间指纹认证单元
指纹范本
6
解密密钥
7
认证接口单元
送认证的授权密钥
5'
认证的解密密钥
7'
304

图5

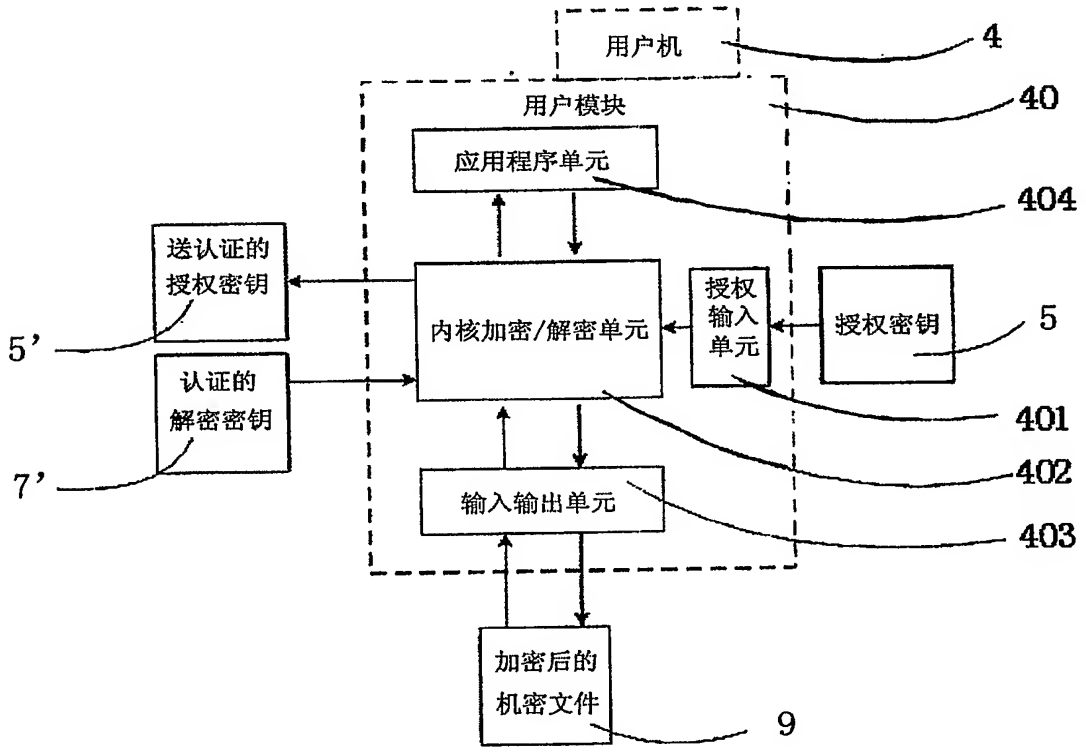

用户机
4
用户模块
40
应用程序单元
404
送认证的授权密钥
5'
认证的解密密钥
7'
内核加密/解密单元
授权输入单元
授权密钥
5
401
402
输入输出单元
403
加密后的机密文件
9

图6

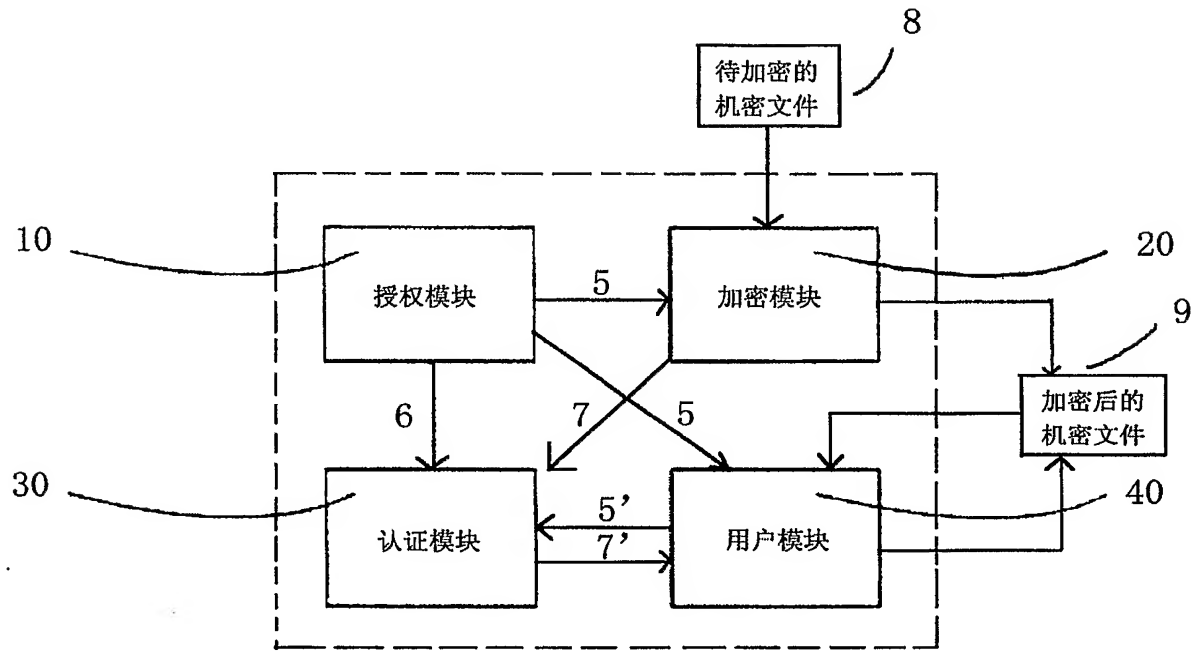


图7